TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

(chapitre II du Traité de coopération en matière de brevets)

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE À DONNER** voir formulaire PCT/IPEA/416	
Demande internationale No. PCT/EP2004/051198	Date du dépôt international *(jour/mois/année)* 22.06.2004	Date de priorité *(jour/mois/année)* 25.06.2003
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant NAGRACARD S.A. ET AL.		

1. Le présent rapport est le rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international en vertu de l'article 35 et transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.
3. Ce rapport est accompagné d'ANNEXES, qui comprennent :
   a. ☒ un total de *(envoyées au déposant et au Bureau international)* 3 feuilles, définies comme suit :
      ☐ les feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou des feuilles contenant des rectifications autorisées par la présente administration (voir la règle 70.16 et l'instruction administrative 607).
      ☒ des feuilles qui remplacent des feuilles précédentes, mais dont la présente administration considère qu'elles contiennent une modification qui va au-delà de l'exposé de l'invention qui figure dans la demande internationale telle qu'elle a été déposée, comme il est indiqué au point 4 du cadre n° I et dans le cadre supplémentaire.
   b. ☐ *(envoyées au Bureau international seulement)* un total de (préciser le type et le nombre de support(s) électronique(s)) , qui contiennent un listage de la ou des séquences ou un ou des tableaux y relatifs, déposés sous forme déchiffrable par ordinateur seulement, comme il est indiqué dans le cadre supplémentaire relatif au listage de la ou des séquences (voir l'instruction administrative 802).

4. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

☒	Cadre n° I	Base de l'opinion
☒	Cadre n° II	Priorité
☐	Cadre n° III	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
☐	Cadre n° IV	Absence d'unité de l'invention
☒	Cadre n° V	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
☐	Cadre n° VI	Certains documents cités
☐	Cadre n° VII	Irrégularités dans la demande internationale
☐	Cadre n° VIII	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
15.04.2005	18.08.2005
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Rachkov, V N° de téléphone +31 70 340-4953

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

Demande internationale n°
PCT/EP2004/051198

Case No. I Base du rapport

1. En ce qui concerne la **langue**, le présent rapport est établi sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous ce point.

   ☐ Le présent rapport est établi sur la base de traductions réalisées à partir de la langue d'origine dans la langue suivante ,qui est la langue d'une traduction remise aux fins de :
   - ☐ la recherche internationale (selon les règles 12.3 et 23.1.b))
   - ☐ la publication de la demande internationale (selon la règle 12.4)
   - ☐ l'examen préliminaire international (selon la règle 55.2 ou 55.3)

2. En ce qui concerne les **éléments*** de la demande internationale, le présent rapport est établi sur la base des éléments suivants (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport.*) :

Description, Pages	
1-7	telles qu'initialement déposées
Revendications, No.	
1-12	reçue(s) le 15.04.2005 avec lettre du 12.04.2005
Dessins, Feuilles	
1/2, 2/2	telles qu'initialement déposées

☐ En ce qui concerne un listage de la ou des séquences ou un ou des tableaux y relatifs, voir le cadre supplémentaire relatif au listage de la ou des séquences.

3. ☐ Les modifications ont entraîné l'annulation :
   - ☐ de la description, pages
   - ☐ des revendications, nos
   - ☐ des dessins, feuilles/fig.
   - ☐ du listage de la ou des séquences *(préciser)* :
   - ☐ d'un ou de tous les tableaux relatifs au listage de la ou des séquences *(préciser)* :

4. ☒ Le présent rapport a été établi abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué dans le cadre supplémentaire (règle 70.2.c)).
   - ☐ de la description, pages
   - ☒ des revendications, nos 1-12
   - ☐ des dessins, feuilles/fig.
   - ☐ du listage de la ou des séquences *(préciser)* :
   - ☐ d'un ou de tous les tableaux relatifs au listage de la ou des séquences *(préciser)* :

** Si le cas visé au point 4 s'applique, certaines ou toutes ces feuilles peuvent être revêtues de la mention "remplacé".*

RAPPORT PRÉLIMINAIRE INTERNATIONAL SUR LA BREVETABILITÉ

Demande internationale n°
PCT/EP2004/051198

Case No. II Priorité

1. ☐ Le présent rapport a été formulée comme si aucune priorité n'avait été revendiquée, du fait que les documents suivants n'ont pas été remis dans le délai prescrit :
   - ☐ copie de la demande antérieure dont la priorité a été revendiquée (règle 66.7.a))
   - ☐ traduction de la demande antérieure dont la priorité a été revendiquée (règle 66.7.b))

2. ☐ Le présent rapport a été établi comme si aucune priorité n'avait été revendiquée, du fait que la revendication de priorité a été jugée non valable (règle 64.1). Pour les besoins du présent rapport, la date de dépôt international indiquée plus haut est donc considérée comme la date pertinente.

3. Observations complémentaires, le cas échéant :

   voir feuille séparée

Cadre n° V Déclaration motivée selon l?article 35.2) quant à la nouveauté, l?activité inventive et la possibilité d?application industrielle; citations et explications à l?appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-9
	Non:	Revendications	
Activité inventive	Oui:	Revendications	
	Non:	Revendications	1-9
Possibilité d'application industrielle	Oui:	Revendications	1-9
	Non:	Revendications	

2. Citations et explications (règle 70.7) :

   voir feuille séparée

Concernant le point I
Base de l'opinion

1 Les modifications introduites avec la lettre du 12.04.2005 conduisent à étendre l'objet de la demande au-delà du contenu de la demande telle qu'elle a été déposée. Elles vont par conséquent à l'encontre des dispositions de l'article 34(2) b) PCT. Les modifications concernées sont les suivantes:

a) La revendication 1 définit une étape de "transmission par l'autorité d'au moins la clé publique du fournisseur à l'opérateur". Cette définition n'a pas de fondement dans la demande initiale. D'après la description le fournisseur FO transmet sa clé publique à l'opérateur OP (al. 038) et l'opérateur récupère la clé dans le cas d'une demande de service (al. 040). Cependant, une transmission de la clé publique du fournisseur à l'opérateur par l'autorité n'est mentionnée ni dans la description ni dans les figures. Cette étape ne découle pas directement et sans ambiguïté du fait que l'opérateur récupère "les informations nécessaires" auprès de l'autorité IS. Puisque la clé publique du fournisseur est transmise à l'opérateur (par le fournisseur lui-même), elle ne peut pas être considérée comme une "information nécessaire" que l'opérateur aurait récupéré auprès de l'autorité IS.

b) La revendication 1 définit une étape de "désactivation ou effacement par l'opérateur d'au moins une partie de la zone mémoire dédiée à une ressource". Cette définition n'a pas de fondement dans la demande initiale. D'après la description toute la zone mémoire dédiée à une ressource est effacée (al. 024).

c) D'après la revendication 2 l'étape de désactivation ou effacement consiste à effacer au moins la clé publique du fournisseur. Cette définition n'a pas de fondement dans la demande initiale. D'après la description l'étape de désactivation ou effacement consiste à effacer la clé du fournisseur qui est stockée dans la partie de gestion (comprenant aussi la définition des zones de ressources dédiées) et à effacer toute la zone mémoire dédiée à une ressource.

L'examen préliminaire international ne tient pas compte des modifications qui conduisent à étendre l'objet de la demande au-delà du contenu de la demande telle qu'elle a été déposée (Règle 70.2(c) PCT) ce qui est équivalent, dans le cas du jeu

de revendications présent, à baser l'examen sur les revendications de la demande initiale. Par conséquent, ce rapport fait référence aux revendications 1 à 9 de la demande initiale.

Concernant le point II
Priorité

1 Les passages de la description sur lesquels se fonde la revendication 9 ne font pas partie de la demande dont la priorité est revendiquée (EP03014209). En conséquence, la priorité revendiquée ne peut pas être accordée à la revendication 9.

Concernant le point V
Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1 Il est fait référence aux documents suivants dans ce rapport:
D1 : US 6 385 723 B1 (RICHARDS TIMOTHY PHILIP) 7 mai 2002 (2002-05-07)
D2 : EP 0 973 135 A (SONY CORP) 19 janvier 2000 (2000-01-19)

2 La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT pour les raisons suivantes:.

2.1 Le document D1 décrit une méthode d'allocation de ressources d'un module de sécurité d'un appareil connecté à un réseau (col. 5, lignes 51-55), ce réseau étant administré par un opérateur (col. 4, lignes 30-35 et col. 5, lignes 51-55), lesdites ressources étant utilisées par des fournisseurs d'application (col. 5, lignes 49-51), cette méthode consistant dans les étapes suivantes:
-génération d'une paire de clés asymétriques et stockage de la clé privée dans le module de sécurité, la clé publique étant stockée chez une autorité (col. 7, lignes 45-54 et col. 8, lignes 45-47),
-introduction d'au moins une clé publique de l'autorité dans le module de sécurité (col. 10, lignes 19-20),

-réception par l'autorité d'une requête d'un fournisseur, cette requête comprenant au moins la clé publique du fournisseur (col. 9, lignes 37-40),
-transmission par l'autorité (par l'intermédiaire du fournisseur) d'une instruction de réservation de ressources vers le module de sécurité, accompagnée par la clé publique du fournisseur (col. 6, lignes 28-34, col. 9, lignes 37-49 et col. 10, lignes 22-28),
-transmission par l'autorité de la clé publique du module de sécurité au fournisseur (col. 8, lignes 45-47 et col. 11, lignes 3-7),
-établissement d'une communication sécurisée entre le fournisseur et le module de sécurité (col. 10, al. 48-52).
-chargement d'une application par le fournisseur dans le module de sécurité (col. 10, al. 48-52).

Note: D'après le document D1 l'appareil connecté à un réseau est un terminal ATM (guichet bancaire automatique). Il est implicite que le terminal ATM est connecté à un réseau bancaire qui est administré par une banque. Cette banque est donc l'opérateur de ce réseau.

Par conséquent, l'objet de la revendication 1 diffère de cette méthode d'allocation de ressources connue en ce que l'opérateur sert d'intermédiaire dans les interactions et communique directement avec le module de sécurité (ce qui permet l'allocation d'une ressource spécifique désignée par l'opérateur).

Note: En effet, si l'autorité et l'opérateur étaient considérés comme une même entité (comme indiqué dans la présente demande, les fonctions de l'autorité peuvent être assumées par l'opérateur, par exemple une banque), les échanges entre le fournisseur, le module de sécurité et cette entité, tels que décrits dans le document D1, auraient été identiques aux échanges définis par la revendication 1. La différence entre la méthode du document D1 et celle définie par la revendication 1 consiste donc en la répartition des fonctions entre l'opérateur et l'autorité.

Compte tenu de la méthode décrite dans le document D1, la personne du métier est confrontée au problème de fournir à l'opérateur les moyens permettant de contrôler de manière précise l'allocation de ressources dans le module de sécurité. Pour résoudre le problème posé, la personne du métier considérerait le document D2 dans le même domaine d'allocation sécurisée de ressources. Le document D2 décrit une méthode d'allocation d'après laquelle l'émetteur du module de sécurité joue un rôle d'intermédiaire dans les interactions et adresse directement à la carte les instructions nécessaires pour l'allocation d'une ressource spécifique (col. 16, al. 110 et fig. 7). Compte tenu de cette information, la personne du métier adapterait la méthode du document D1 en sorte que l'émetteur du module de sécurité (l'opérateur) joue un rôle d'intermédiaire dans les interactions et qu'il transmette une instruction de

réservation d'une ressource spécifique vers le module de sécurité et obtenir ainsi l'objet de la revendication 1 sans qu'une activité inventive soit impliquée (article 33(3) PCT).

2.2 Les revendications dépendantes contiennent des caractéristiques qui représentent des détails d'implémentation ou des possibilités évidentes que la personne du métier pourrait choisir, selon le cas d'espèce, sans impliquer d'activité inventive. Aucune de ces caractéristiques, combinée avec les caractéristiques d'une quelconque revendication à laquelle les revendications mentionnées ci-dessus se réfèrent, ne satisfait aux exigences du PCT en matière d'activité inventive (article 33(3) PCT).

REVENDICATIONS

1. Méthode d'allocation de ressources d'un module de sécurité d'un appareil connecté à un réseau, ce réseau étant administré par un opérateur (OP), lesdites ressources (RSC) étant utilisées par des fournisseurs d'application (FO), cette méthode consistant dans les étapes suivantes :

- génération d'une paire de clés asymétriques et stockage de la clé privée dans le module de sécurité (US-SM), la clé publique (KPuUS) étant stockée chez une autorité (IS),
- introduction d'au moins une clé publique de l'autorité (KPuIS) dans le module de sécurité (US-SM),
- réception par l'opérateur (OP) d'une requête d'un fournisseur (FO) et transmission de cette requête à l'autorité (IS), cette requête comprenant au moins la clé publique du fournisseur (KPuFO),
- **transmission par l'autorité (IS) d'au moins la clé publique du fournisseur (KpuFO) à l'opérateur (OP),**
- transmission par l'opérateur (OP) d'une instruction de réservation d'une ressource (RSC) vers le module de sécurité (US-SM) accompagnée par la clé publique du fournisseur (KPuFO),
- transmission par l'opérateur (OP) de la clé publique (KPuUS) du module de sécurité au fournisseur (FO),
- établissement d'une communication sécurisée entre le fournisseur (FO) et le module de sécurité (US-SM),
- chargement d'une application par le fournisseur (FO) dans le module de sécurité (US-SM).
- **désactivation ou effacement par l'opérateur (OP) d'au moins une partie de la zone mémoire dédiée à une ressource déterminée lorsque les conditions d'effacement sont remplies.**

2. Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que l'étape de désactivation ou effacement d'au moins une partie de la zone

mémoire dédiée à une ressource déterminée consiste à effacer au moins la clé publique du fournisseur (KpuFO).

3. Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que les conditions d'effacement sont remplies lorsque la ressource a été exécutée un nombre de fois égal ou supérieur à un nombre limité prédéterminé.

4. Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que les conditions d'effacement sont remplies lorsque la ressource a été exécutée pendant un temps égal ou supérieur à un temps limité prédéterminé.

5. Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que la paire de clés asymétriques est générée par le module de sécurité, la clé publique étant alors transmise à l'autorité.

6. Méthode d'allocation de ressources selon la revendication 1, caractérisé en ce que des paramètres d'initialisation d'une clé de session (M, b) propre à l'opérateur sont stockés dans les modules de sécurité lors de l'initialisation.

7. Méthode d'allocation de ressources selon les revendications 1 à 6, caractérisée en ce que le fournisseur transmet des paramètres d'initialisation d'une clé de session (M, b) à l'opérateur, ces paramètres étant transmis au module de sécurité lors de la réservation d'une ressource.

8. Méthode d'allocation de ressources selon les revendications 1 à 7, caractérisée en ce que l'établissement d'une communication sécurisée entre le fournisseur et le module de sécurité est basé sur l'utilisation de la clé publique du fournisseur par le module de sécurité et par l'utilisation de la clé publique du module de sécurité par le fournisseur.

9. Méthode d'allocation de ressources selon la revendication 6, caractérisée en ce que l'établissement d'une communication sécurisée entre l'opérateur et le module de sécurité est basé sur la génération d'une clé de session utilisant les paramètres d'initialisation (M, b) de l'opérateur.

10. Méthode d'allocation de ressources selon la revendication **7**, caractérisée en ce que l'établissement d'une communication sécurisée entre le fournisseur et le module de sécurité est basé sur la génération d'une clé de session utilisant les paramètres d'initialisation (M, b) du fournisseur.

11. Méthode d'allocation de ressources selon l'une des revendications précédentes, caractérisée en ce que l'autorité (IS) et l'opérateur (OP) forment une même entité.

12. Méthode d'allocation de ressources selon l'une des revendications précédentes, caractérisée en ce que l'instruction de réservation d'une ressource (RES) comprend l'envoi d'une clé de domaine (DK) spécifique à une application et commune à tous les modules de sécurité disposant de cette application, cette clé étant utilisée pour l'établissement de la communication sécurisée entre le fournisseur FO et le module de sécurité.